

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Please amend claims 1, 2, 4-9, 12-34, 36, 37, 39-50 and 52-54 as follows:

1. (Currently Amended) A method of detecting unauthorized access attempts to a network, comprising:

receiving a request from a user to obtain an address;

obtaining said address;

generating a substitute return address corresponding to output of a function applied to said address, said substitute return address corresponding to a used one of a block of substitute addresses;

returning said substitute return address to said user;

monitoring access to said address; and

detecting an unauthorized attempt to access said address when an attempted address corresponds to an unused one of said block of substitute addresses.

2. (Currently Amended) The method according to claim 1, wherein said function further comprises hashing a user address of said user to obtain one value of a range of values mapping to said block of substitute addresses, said one value designating said used one of said block of substitute addresses.

3. (Previously Amended) The method according to claim 2, wherein said function further comprises hashing a time of said request.

4. (Currently Amended) The method according to claim 2, wherein detecting comprises tracing said user when said attempted address corresponds to said unused one of said block of substitute addresses.

5. (Currently Amended) The method according to claim 4, comprising blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

6. (Currently Amended) The method according to claim 4, wherein unused ones of said block of substitute addresses correspond to attack detectors.
7. (Currently Amended) The method according to claim 1, wherein said function further comprises hashing a time of said request to obtain one value of a range of values mapping to said block of substitute addresses, said one value designating said used one of said block of substitute addresses.
8. (Currently Amended) The method according to claim 1, wherein said function further comprises changing said used one of said block of substitute addresses over time.
9. (Currently Amended) The method according to claim 8, wherein said function further comprises determining a time period for changing said one of said block of substitute addresses.
10. (Previously Presented) The method according to claim 9, wherein determining the time period comprises using a pre-selected time period.
11. (Previously Presented) The method according to claim 9, wherein determining the time period comprises generating a random time period.
12. (Currently Amended) The method according to claim 8, wherein changing said used one of said block of substitute addresses comprises randomly choosing said used one from said block of substitute addresses.
13. (Currently Amended) The method according to claim 8, wherein detecting comprises tracing said user when said attempted address corresponds to said unused one of said block of substitute addresses.
14. (Currently Amended) The method according to claim 13, comprising blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

15. (Currently Amended) The method according to claim 13, wherein unused ones of said block of substitute addresses correspond to attack detectors.

16. (Currently Amended) The method according to claim 8, further comprising determining said attempt is authorized when a connection exists between said user and said unused ~~address~~ one of said block of substitute addresses.

17. (Currently Amended) The method according to claim 8, wherein changing said used one of said block of substitute addresses comprises coordinating changes in a name-to-address database and a host identity-to-address database.

18. (Currently Amended) The method according to claim 1, wherein detecting comprises tracing said user when said attempted address corresponds to said unused one of said block of substitute addresses.

19. (Currently Amended) The method according to claim 18, comprising blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

20. (Currently Amended) The method according to claim 1, wherein unused ones of said block of substitute addresses correspond to attack detectors.

21. (Currently Amended) A computer-readable medium containing instructions for controlling a processor to detect unauthorized access attempts to a network by:

- receiving a request from a user to obtain an address;
- obtaining said address;
- generating a substitute return address corresponding to output of a function applied to said address, said substitute return address corresponding to a used one of a block of substitute addresses;
- returning said substitute return address to said user;
- monitoring access to said address; and

detecting an unauthorized attempt to access said address when an attempted address corresponds to an unused one of said block of substitute addresses.

22. (Currently Amended) The computer-readable medium of claim 21, further comprising instructions for controlling the processor to apply said function by hashing at least one of a user address of said user and a time of said request to obtain one value of a range of values mapping to said block of substitute addresses, said one value designating said used one of said block of substitute addresses.

23. (Currently Amended) The computer-readable medium of claim 21, further comprising instructions for controlling the processor to detect said unauthorized attempt by tracing said user when said attempted address corresponds to said unused one of said block of substitute addresses.

24. (Currently Amended) The computer-readable medium of claim 23, further comprising instructions for controlling the processor to detect said unauthorized attempt by blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

25. (Currently Amended) The computer-readable medium of claim 21, further comprising instructions for controlling the processor to apply said function by changing said used one of said block of substitute addresses over time.

26. (Currently Amended) The computer-readable medium of claim 25, further comprising instructions for controlling the processor to change said used one of said block of substitute addresses over time by at least one of determining a time period using a pre-selected time period and determining a time period by generating a random time period.

27. (Currently Amended) The computer-readable medium of claim 25, further comprising instructions for controlling the processor to change said used one of said block of substitute addresses by randomly choosing said used one from said block of substitute addresses.

28. (Currently Amended) The computer-readable medium of claim 25, further comprising instructions for controlling the processor to determine said attempt is authorized by determining that a connection exists between said user and said unused ~~address~~ one of said block of substitute addresses.

29. (Currently Amended) The computer-readable medium of claim 25, further comprising instructions for controlling the processor to change said used one of said block of substitute addresses by coordinating changes in a name-to-address database and a host identity-to-address database.

30. (Currently Amended) A system for detecting unauthorized access attempts to a network, comprising:

means for receiving a request from a user to obtain an address;

means for obtaining said address;

means for generating a substitute return address corresponding to output of a function applied to said address, said substitute return address corresponding to a used one of a block of substitute addresses, said means for generating including a processor programmed to apply said function to said address;

means for returning said substitute return address to said user;

means for monitoring access to said address; and

means for detecting an unauthorized attempt to access said address when an attempted address corresponds to an unused one of said block of substitute addresses.

31. (Currently Amended) The system of claim 30, wherein said means for generating further comprises means for hashing at least one of a user address of said user and a time of said request to obtain one value of a range of values mapping to said block of substitute addresses, said one value designating said used one of said block of substitute addresses.

32. (Currently Amended) The system of claim 30, wherein said means for detecting further comprise means for tracing said user when said attempted address corresponds to said unused one of said block of substitute addresses.

33. (Currently Amended) The system of claim 32, wherein said means for detecting further comprise means for blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

34. (Currently Amended) The system of claim 30, wherein said means for generating further comprise means for changing said used one of said block of substitute addresses over time.

35. (Original) The system of claim 34, wherein said means for changing further comprise at least one of means for determining a time period using a pre-selected time period and means for determining a time period by generating a random time period.

36. (Currently Amended) The system of claim 34, wherein said means for changing further comprise means for randomly choosing said used one from said block of substitute addresses.

37. (Currently Amended) The system of claim 34, further comprising means for determining said attempt is authorized when a connection exists between said user and said unused ~~address~~ one of said block of substitute addresses.

38. (Original) The system of claim 34, further comprising:
a name-to-address database;
a host identity-to-address database; and
means for coordinating changes in said name-to-address database and said host identity-to-address database in conjunction with said means for changing.

39. (Currently Amended) A computer program, disposed on a computer-readable medium, for enabling detection of unauthorized access attempts to a network, said computer program including instructions for causing a processor to:
receive a request from a user to obtain an address;
obtain said address;
generate a substitute return address corresponding to output of a function applied to said address, said substitute return address corresponding to a used one of a block of substitute addresses;

return said substitute return address to said user;
monitor access to said address; and
detect an unauthorized attempt to access said address when an attempted address corresponds to an unused one of said block of substitute addresses.

40. (Currently Amended) The computer program of claim 39, wherein said instructions for causing the processor to generate said substitute return address further include instructions for causing a processor to at least one of hash a user address of said user and hash a time of said request to obtain one value of a range of values mapping to said block of substitute addresses, said one value designating said used one of said block of substitute addresses.

41. (Currently Amended) The computer program of claim 40, wherein said instructions for causing the processor to detect further include instructions for causing a processor to trace said user when said attempted address corresponds to said unused one of said block of substitute addresses.

42. (Currently Amended) The computer program of claim 41, further including instructions for causing the processor to block additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

43. (Currently Amended) The computer program of claim 41, further including instructions for causing the processor to correspond said unused ones of said block of substitute addresses with attack detectors.

44. (Currently Amended) The computer program of claim 39, wherein said instructions for causing the processor to generate said substitute return address further include instructions for causing a processor to change said used one of said block of substitute addresses over time.

45. (Currently Amended) The computer program of claim 44, wherein said instructions for causing the processor to generate said substitute return address further include instructions for causing a processor to at least one of use a pre-selected time period for changing said one of said block of substitute addresses and generate a random time period for changing said one of

said block of substitute addresses.

46. (Currently Amended) The computer program of claim 44, wherein said instructions for causing the processor to change said used one of said block of substitute addresses further include instructions for causing a processor to randomly choose said used one from said block of substitute addresses.

47. (Currently Amended) The computer program of claim 44, wherein said instructions for causing the processor to detect further include instruction for causing a processor to trace said user when said attempted address corresponds to said unused one of said block of substitute addresses.

48. (Currently Amended) The computer program of claim 47, further including instructions for causing the processor to block additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

49. (Currently Amended) The computer program of claim 47, further including instructions for causing the processor to correspond attack detectors with unused ones of said block of substitute addresses.

50. (Currently Amended) The computer program of claim 44, further including instructions for causing the processor to determine said attempt is authorized when a connection exists between said user and said unused ~~address~~ one of said block of substitute addresses.

51. (Previously Presented) The computer program of claim 44, further including instructions for causing the processor to coordinate said change in a name-to-address database and a host identity-to-address database.

52. (Currently Amended) The computer program of 39, wherein said instructions for causing the processor to detect further include instructions for causing a processor to trace said user when said attempted address corresponds to said unused one of said block of substitute addresses.

53. (Currently Amended) The computer program of claim 52, further including instructions for causing the processor to block additional unauthorized attempts when said attempted address corresponds to said unused one of said block of substitute addresses.

54. (Currently Amended) The computer program of claim 39, further including instructions for causing the processor to correspond attack detectors with unused ones of said block of substitute addresses.